OWASP

Open Web Application Security Project

业务数据安全实践

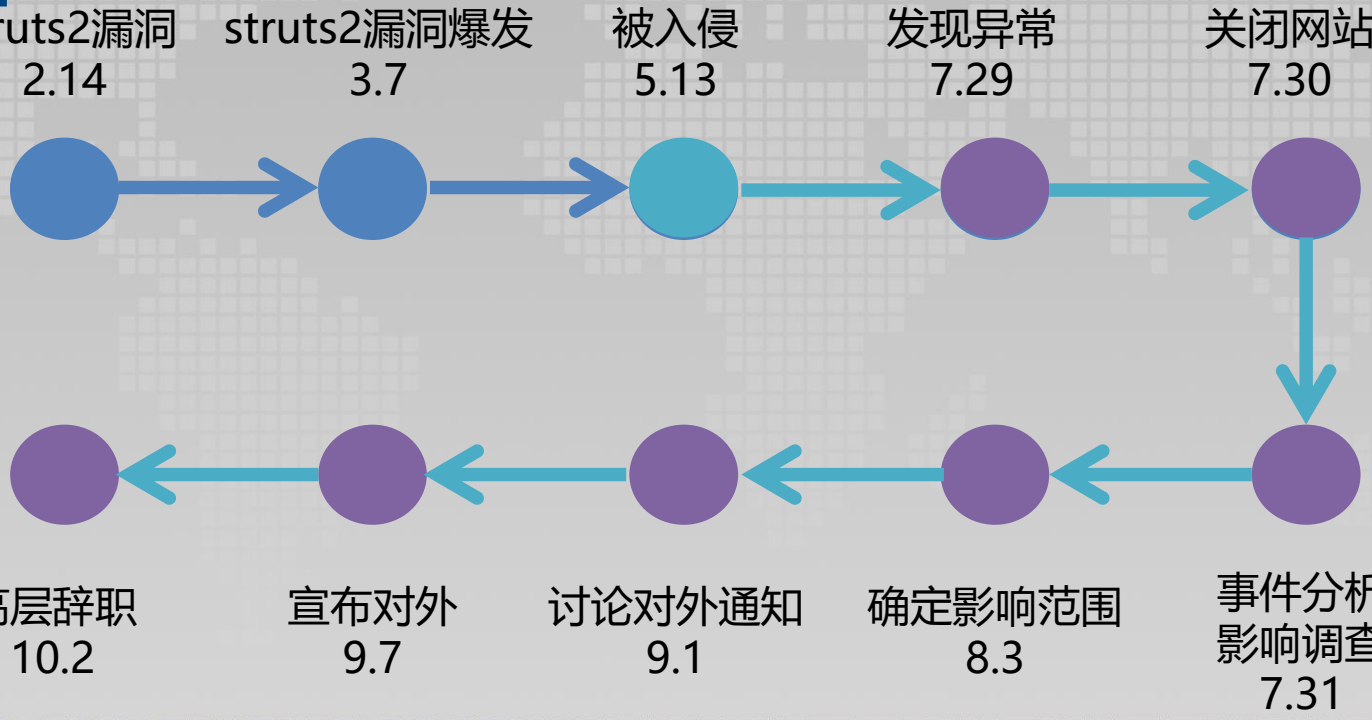
廖威

背景

2018年数据泄露事件一隅

1. Aadhaar——10亿条
2. 圆通——10亿
3. 华住——5亿
4. UnderArmour——1.5亿
5. MyHeritage——9200万
6. Facebook——8700万
7. Panera——3700万
8. Ticketfly——2700万
9. Sacramento Bee——1950万
10. AcFun——800万

Equifax数据泄漏



目录

数据安全感悟

数据分类

数据加密

分类分级
全面加密

持续整改

数据安全感悟

1.未雨绸缪
　　提前做好制度技术储备

2.自上而下与自下而上结合
　　尚方宝剑

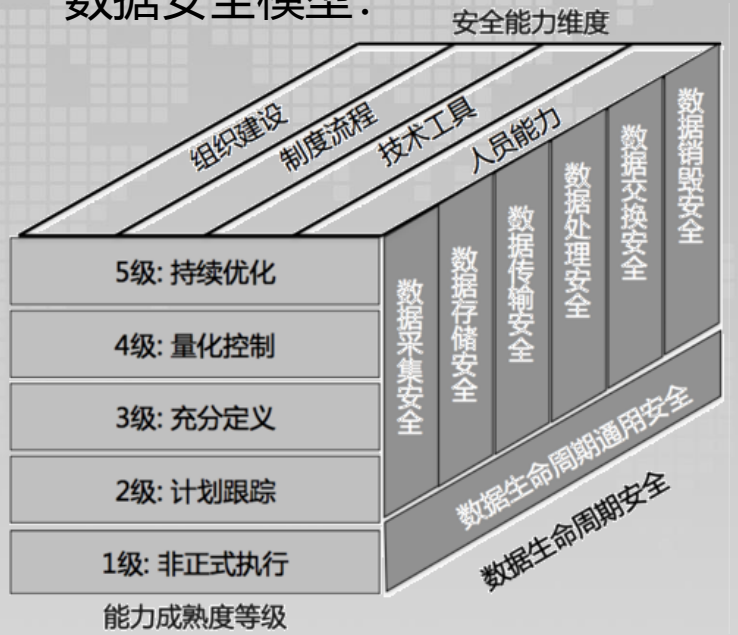
3.天时地利
　　风险上报、合规检查

数据安全

数据安全原则：

- ✓ 进不来
- ✓ 拿不走
- ✓ 看不懂
- ✓ 改不了
- ✓ 走不脱

数据安全模型：



目录

1.数据安全感悟

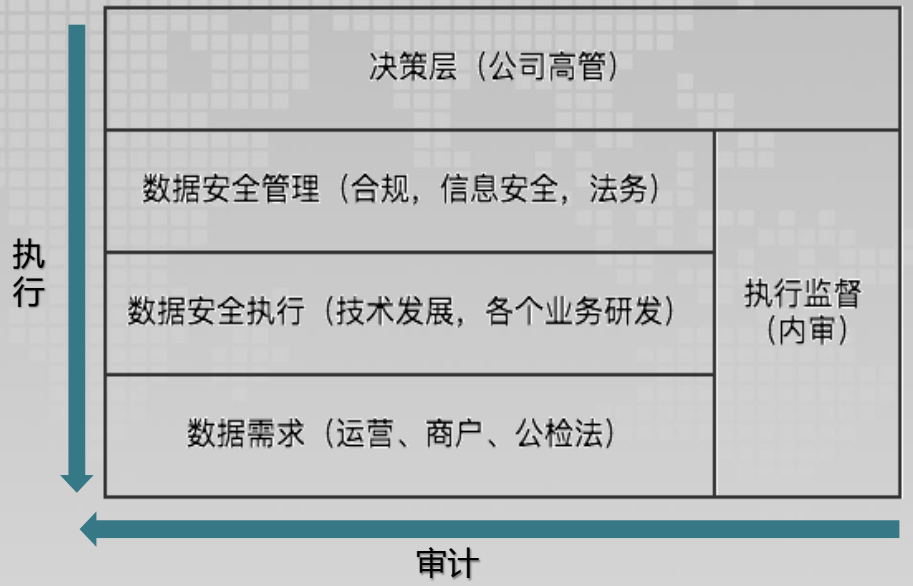
2.数据安全组织与管理

3.数据安全人员与技术

数据安全组织与管理

公司高管重视数据安全

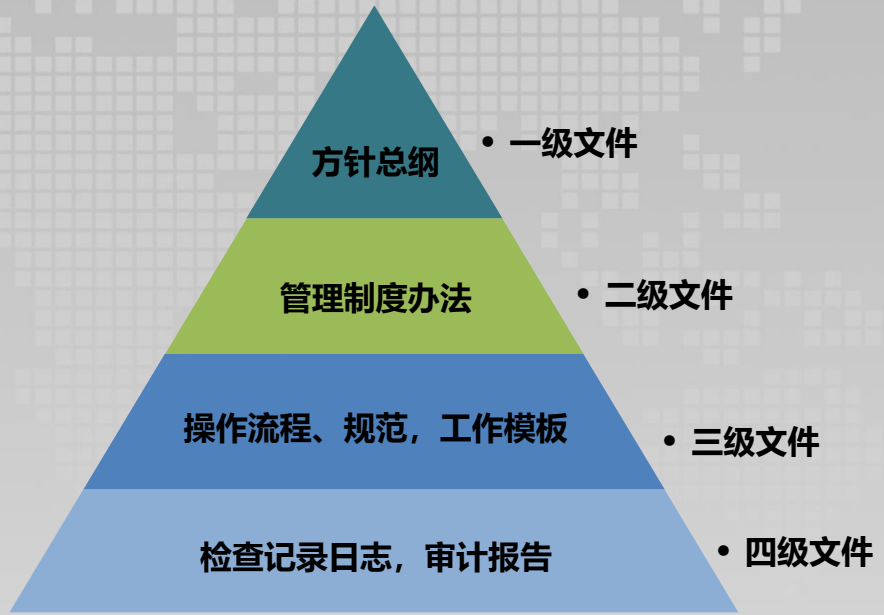
自上而下实施数据策略



数据安全组织与管理

参考 ISO 27001

建立数据安全管理体系



目录

数据安全技术与人员

数据保护原则：纵深防御

数据的生命周期一般分为：

- 采集
- 传输
- 存储
- 处理
- 交换
- 销毁

数据安全：数据采集

数据采集为实现支付交易、金融认证授权、风险控制、信用服务等目的，对敏感数据进行获取和记录的过程。

1.数据采集规则

采集目的、用途、方式、范围，是否合规授权

2.数据采集防护

安全措施：敏感数据需要加密；防止第三方攻击

3.数据分类分级

根据数据被泄露或修改后对用户或公司造成的影响程度，分为两类三级

数据安全：数据采集

数据分级表

分级	名称	类别	举例
L2	二级数据	L2.1密码信息	登录密码、支付密码、取款密码 、密码提示问题答案等
		L2.2非生物认证信息	法定证件图片（如身份证图片）、有效期内的身份验证Token/凭证等
		L2.3生物认证信息	虹膜、耳纹、掌纹、静脉、指纹、人脸、声纹、眼纹、步态、笔迹等
		L2.4银行卡相关数据	银行卡的CVV 、有效期、PIN码、磁道信息等
		L2.5联系信息	手机号、电话号、详细地址、姓名、社交网络账号、邮箱、地址簿等
		L2.6唯一识别信息	法定证件（如身份证、护照、驾驶证等）号码及有效期限
		L2.7账户信息	账号和卡号、账户开立时间、开户行、账户余额、账户交易情况等
L1	一级数据	L1.1推演性凭证信息	替代账号、卡号的标记化Token凭证等
		L1.2个人基本信息	性别、国籍、民族、职业、婚姻状况、家庭状况、住所或工作单位地址及照片等
		L1.3个人金融交易信息	支付记录、金融相关浏览记录、贷款记录、信用卡使用记录等
		L1.4个人信用信息	信用卡还款情况、贷款偿还情况以及个人在经济活动中形成的，能够反映其信用状况的其他信息等
		L1.5个人财产信息	个人收入状况、拥有的不动产状况、拥有的车辆状况、纳税额、公积金缴存金额等
		L1.6衍生信息	对个人消费习惯、投资意愿、支付习惯等原始信息进行处理、分析所形成的反映特定个人某些情况的信息
		L1.7个人网络环境信息	客户端IP、MAC、IMEI、IMSI、Wi-Fi、地理位置定位等
L0	零级数据	L0.1社交信息	昵称、签名档、社交网络头像等
		L0.2脱敏的信息	只展示前3后4的手机号、前4后2的身份证号等

数据安全：数据传输

数据传输是已获取的数据在已获授权机构或企业的系统内或系统间转移的过程。安全传输需保障数据：保密性，完整性，抗抵赖。

1.网络层

ipsec VPN、专线

2.传输层

HTTPS/TLS

3.应用层

端到端加密

数据安全：数据存储

数据存储是指已获取的数据在已获授权机构或企业的系统内保存的过程。安全存储需保障数据：保密性、完整性、可用性。

1.数据存储加密方式

物理所在地、数据标签、分层加密

2.加密密钥管理

三级密钥管理体系

3.加密算法使用

三种加密算法使用

数据安全：数据存储

数据存储分层加密，确保每层数据被攻破，数据还是保密的。

1.操作系统层

使用硬件或软件对OS级别进行透明加密

2.分区层

对某个分区进行加密

3.应用层

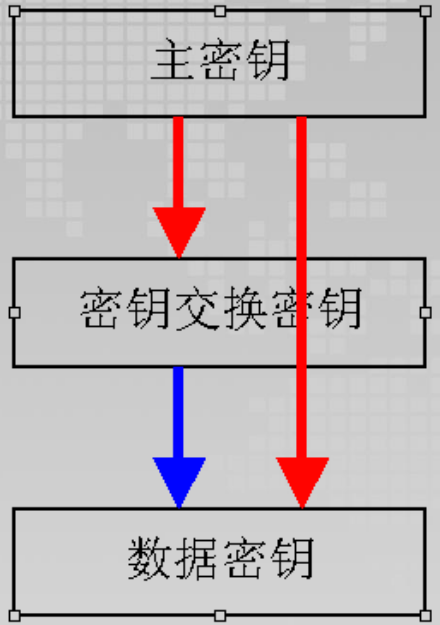
对数据库文件进行加密

4.业务层

对业务数据一组一密

数据安全：数据存储之密钥

数据安全加密核心在于：密钥与算法。加密一般建议使用公开算法，通过密钥的私密性确保数据安全。我们使用三级密钥管理体系管理密钥以及解决加密数据搜索问题。



1.密钥加密管理

2.密钥定期更换

3.密钥授权与审计

数据安全：数据存储之算法

加密算法一般分为三种

1.对称算法（AES）
　　数据加密

2.非对称算法（公开加密算法 RSA）
　　数据加密、身份认证、数字签名

3.单向散列算法（哈希算法 SHA512RSA，Argon2）
　　文件校验、鉴权、防篡改

数据安全：数据存储之算法

加密算法的模式有：ECB，CBC，CFB，OFB

加密明文在64位以内，使用ECB，超过64位，使用CBC、CFB、 OFB
若是不清楚，则使用CBC

Table 1

	EBC	CBC	CFB	OFB
优点	1.简单； 2.有利于并行计算； 3.误差不会被传送；	1.不容易主动攻击,安全性好于ECB,适合传输长度长的报文,是TLS、IPSec的标准。	1、隐藏了明文模式； 2、分组密码转化为流模式； 3、可以及时加密传送小于分组的数据。	1、隐藏了明文模式； 2、分组密码转化为流模式； 3、可以及时加密传送小于分组的数据。
缺点	1.不能隐藏明文的模式； 2.可能对明文进行主动攻击。	1、不利于并行计算； 2、误差传递； 3、需要初始化向量IV。	1、不利于并行计算； 2、误差传送：一个明文单元损坏影响多个单元； 3、唯一的IV。	1、不利于并行计算； 2、对明文的主动攻击是可能的； 3、误差传送：一个明文单元损坏影响多个单元。

数据安全：数据存储之算法

Zeros填充	X923 填充	ISO10126 填充
全部填充为0的字节	填充为0的字节序列，最后一个字节记录填充的总字节数	填充随机字节序列，最后一个字节记录填充的总字节数
F1 F2 F3 F4 F5 F6 F7 F8 //第一块 F9 00 00 00 00 00 00 00 //第二块	F1 F2 F3 F4 F5 F6 F7 F8 //第一块 F9 00 00 00 00 00 00 07 //第二块	F1 F2 F3 F4 F5 F6 F7 F8 //第一块 F9 7D 2A 75 EF F8 EF 07 //第二块

PKCS5 填充	PKCS7 填充
每个填充的字节都记录了填充的总字节数，数据为整数倍，也会padding一个块	每个填充的字节都记录了填充的总字节数
F1 F2 F3 F4 F5 F6 F7 F8 //第一块 F9 07 07 07 07 07 07 07 //第二块	F1 F2 F3 F4 F5 F6 F7 F8 //第一块 F9 07 07 07 07 07 07 07 //第二块

数据安全：数据存储之算法

加密算法总结

tag	hash加密	对称加密	非对称加密
用途	1.用户密码存储 2.数据防篡改 3.保证数据完整性	数据加密，保证数据的机密性	1.不可信网络建立可信传输 2.身份认证，防抵赖
算法&位数	SHA 512bit SM3	AES 256bit SM4	RSA 2048bit SM2
注意事项	1.密码加盐，一户一盐； 2.Hmac验签时，需要确保KEY的长度，复杂度；	1.一户一个KEY； 2.定时提醒用户修改KEY	1.所有业务使用HTTPS； 2.若业务特殊需要，建议使用加密机或专有服务器，设备运算

数据安全：数据存储之坑

jdk默认不支持AES 256，需先做系统变更

```
/**
 * 使用AES 算法 加密，默认模式 AES/CBC/PKCS5Padding
 */
static void method3(String str) throws Exception {
    cipher = Cipher.getInstance(CIPHER_ALGORITHM_CBC);
    //KeyGenerator 生成aes算法密钥
    KeyGenerator kg = KeyGenerator.getInstance(KEY_ALGORITHM);
    // JAVA AES 默认为 128bit 需要改为 256位
    kg.init(256);
    secretKey = kg.generateKey();

    System.out.println("密钥的长度为: " + secretKey.getEncoded().length);
```

```
/Library/Java/JavaVirtualMachines/jdk1.8.0_91.jdk/Contents/Home/bin/java ...
密钥的长度为: 32
Exception in thread "main" java.security.InvalidKeyException: Illegal key size
    at javax.crypto.Cipher.checkCryptoPerm(Cipher.java:1039)
    at javax.crypto.Cipher.implInit(Cipher.java:805)
    at javax.crypto.Cipher.chooseProvider(Cipher.java:864)
    at javax.crypto.Cipher.init(Cipher.java:1396)
```

数据安全：数据存储之整改

整改历程：

1.总监沟通会

2.技术碰头会

3.业务洽谈会

4.定时排榜会

数据安全：数据处理与交换

数据处理交换是指对已获取的数据进行加工、利用，对外提供服务的过程。数据处理与交换需确保数据的脱敏，可监控审计。

1.数据监控审计

数据异常审计，行为审计，数据水印

2.数据范围

控制数据处理交换范围

3.数据脱敏

常见Tokenization，掩码，随机伪造

数据安全：数据处理与交换之脱敏

数据脱敏常用掩码事例（缺省保留前3后3）：

敏感信息类型	信息范围	展示规范
银行卡信息	银行卡卡号	显示前 6位 + * （实际位数）+ 后 4 位。 如： 622575******1496
个人信息	1) 身份证号、军官证号、护照号	身份证号： 显示前 4 位 + *（实际位数）+后 2 位，如： 5120**********09 军官证号，护照号： 使用缺省信息隐藏规则
	2）姓名	如果要隐藏，隐藏第一个字
	3）手机号	如需要部分隐藏，区号不算，隐藏中间四位 大陆：显示前 3 位 + **** + 后 4 位。如：137****9050 香港、澳门：显示前2位+****+后2位。如：90****85 台湾：显示前2位+****+后3位。如：90****856 其它海外地区：使用缺省隐藏规则
	4）固定电话号码	如需要部分隐藏，推荐的规范：显示区号和后4位
	5）邮箱	如需要部分隐藏， @前面的字符显示3位，3位后显示3个 *，@后面完整 显示如：con***@163.com 如果少于三位，则全部显示，@前加***，例如 tt@163.com则显示为tt***@163.com

数据安全：数据处理与交换之提取

与合规法务联合制定策略：

1.签署法律知情书

2.vp审批

3.数据提取

4.数据发送

数据安全：数据销毁

数据销毁指对数据进行删除，或对数据存储介质进行消磁、焚烧、粉碎等，使数据不再可获得的过程。

1.数据销毁

剩余信息，内存缓存

2.介质销毁

数据覆盖，消磁，物理销毁

数据安全：人员

数据安全核心在于人。

1.专业技能（专岗）

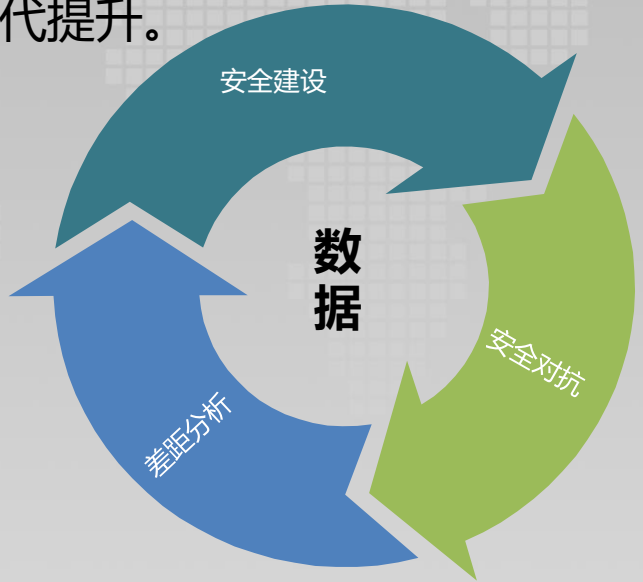
安全管理、技术、运营、合规

2.安全意识（全员）

安全操作意识、安全工作常识

数据安全总结

数据安全建设需要长期持久，需要不断建设验证分析，不断改进，从而实现数据安全能力螺旋式迭代提升。



Thank You

OWASP
Open Web Application Security Project